



دانشکده آموزشهای الکترونیکی

پایان نامه کارشناسی ارشد در رشته مهندسی فناوری اطلاعات (تجارت الکترونیک)

بررسی سیستمهای تشخیص نفوذ در پیاده سازی یک الگوریتم

هوشمند جهت تجارت الکترونیک

توسط:

احمد رضا موذن جهرمی فرد

استاد راهنما:

دکتر منصور ذوالقدری جهرمی

شهریور ماه 1388

بِسْمِ اللّٰهِ الرَّحْمٰنِ الرَّحِیْمِ

به نام خدا

بررسی سیستمهای تشخیص نفوذ در پیاده سازی یک الگوریتم هوشمند

جهت تجارت الکترونیک

به وسیله ی:

احمد رضا موذن جهرمی فرد

پایان نامه

ارائه شده به تحصیلات تکمیلی دانشگاه به عنوان بخشی

از فعالیت های تحصیلی لازم برای اخذ درجه کارشناسی ارشد

در رشته ی :

فناوری اطلاعات

از دانشگاه شیراز

شیراز

جمهوری اسلامی ایران

ارزیابی شده توسط کمیته ی پایان نامه با درجه عالی :

دکتر منصور ذوالقدری جهرمی ، دانشیار بخش مهندسی و علوم کامپیوتر (رئیس کمیته).....

دکتر سراج الدین کاتبی استاد بخش مهندسی و علوم کامپیوتر.....

دکتر محمد هادی صدرالدینی ، دانشیار بخش مهندسی و علوم کامپیوتر.....

شهریور ماه ۱۳۸۸

تقدیم بہ:

مادر عزیز و مہربانم ...

سپاسگزاری

اکنون که بیهاری خداوند متعال موفق به اتمام این پایان نامه شده ام، لازم می دانم از زحمات ارزنده و کجک های بی دریغ استاد کرامت درم جناب آقای دکتر منصور ذوالقدری بزمی که در تمامی مراحل پایان نامه از راهنمایی های ارزشمند خود اینجناب را بهره مند ساختند، قدر دانی کرده و برای ایشان آرزوی سلامتی و موفقیت

کنم.

چکیده

بررسی سیستمهای تشخیص نفوذ در پیاده سازی یک الگوریتم هوشمند

جهت تجارت الکترونیک

به وسیله ی :

احمد رضا موذن

هدف سیستمهای تشخیص نفوذ جلوگیری از دسترسی غیر مجاز کاربران به سایتهای کامپیوتری می باشد. با افزایش بنگاههای تجارت الکترونیکی ، مسئله حفاظت از این سایتهای به یک مانع اساسی در راه توسعه این سیستمها تبدیل شده است. مسئله مهم در این رابطه این است که به مرور زمان روشهای جدیدی برای حمله به سایتهای کامپیوتری طراحی می شوند. در سالهای اخیر از هوش مصنوعی جهت ارتقاء کارایی سیستمهای تشخیص نفوذ استفاده گردیده است. در این پایان نامه ، از سیستمهای دسته بندی فازی جهت معرفی یک سیستم تشخیص نفوذ جدید استفاده شده است. مزیت عمده سیستم پیشنهادی این است که عمل تشخیص مهاجم به کمک مجموعه ای از قوانین فازی انجام می شود که بر ای انسان قابل فهم می باشد. کارائی الگوریتم پیشنهادی با انجام یک سری آزمایش بر روی مجموعه داده KDD99 محاسبه و با چندین روش دیگر که در تحقیقات گذشته پیشنهاد شده مقایسه گردیده است.

فهرست مطالب

صفحه	عنوان
1	1-مقدمه.....
1	1-1-زمینه طرح مسئله.....
2	1-2-تاریخچه سیستم های تشخیص نفوذ.....
8	1-3-مفاهیم اساسی.....
8	1-3-1-تهاجم.....
8	1-3-2-تهدید.....
8	1-3-3-مهاجم.....
9	1-3-4-تشخیص نفوذ.....
9	1-3-5-سیستم تشخیص نفوذ.....
10	1-4-خصوصیات مطلوب سیستم تشخیص نفوذ.....
12	1-5-مشکلات درسیستم های تشخیص نفوذ کنونی.....
14	2-سیستم های تشخیص نفوذ.....
14	2-1-مقدمه.....
14	2-2-انواع تکنیکهای سیستم تشخیص نفوذ.....
14	2-2-1-سیستم تشخیص نفوذ مبتنی بر رفتارهای غیر عادی.....
17	2-2-2-سیستم تشخیص نفوذ مبتنی برعلائم شناسایی.....
17	2-3-تفاوت های سیستم های مبتنی بر رفتار عادی و علائم شناسایی.....
18	2-4-پروفیل چیست؟.....

- 20-2-5- چه زمانی از سیستم تشخیص نفوذ مبتنی بر رفتار عادی استفاده می شود.....
- 21-2-6- موانع استفاده تنها از سیستم تشخیص نفوذ مبتنی بر پایه رفتار غیر عادی.....
- 21-2-7- به چه سطوح کاربردی از حفاظت توجه می شود.....
- 22-2-7-1- سوءاستفاده از پروتکل و سرویس پورت ها.....
- 22-2-7-2- مختل نمودن سرویس سرور توسط داده های ساختگی.....
- 23-2-7-3- مختل نمودن ارائه سرویس از طریق حجم بالای داده.....
- 23-2-7-4- سر ریزشیدن بافر.....
- 24-2-7-5- نواقص ابزارها در شبکه محلی.....
- 24-2-8- انواع سیستم های تشخیص نفوذ.....
- 24-2-8-1- سیستم تشخیص نفوذ مبتنی بر میزبان.....
- 29-2-8-2- سیستم تشخیص نفوذ مبتنی بر شبکه.....
- 3- ابزار های هوشمند جهت طراحی سیستمهای تشخیص نفوذ 35**
- 35-3-1- مقدمه.....
- 37-3-2- الگوریتم ژنتیک.....
- 39-3-3- شبکه های عصبی.....
- 39-3-3-3- یادگیری توسط شبکه های عصبی مصنوعی.....
- 43-3-4- شبکه عصبی-فازی.....
- 43-3-4-1- مقدمه.....
- 44-3-4-2- انواع شبکه های عصبی-فازی.....
- 53-3-5- ماشین بردار پشتیبان.....
- 53-3-5-1- مقدمه.....

54.....	3-5-2- ماشین بردار پشتیبان استاندارد.....
57.....	3-5-3- ماشین بردار پشتیبان در حالت جدایی ناپذیر.....
59.....	3-5-4- ماشین بردار پشتیبان غیر خطی.....
60.....	3-5-5- ماشین بردار پشتیبان در حالت چند کلاسه.....
61.....	3-5-6- ماشین بردار پشتیبان فازی.....
64.....	3-6- بحث و گفتگو.....
65.....	3-7- نتیجه گیری.....
66.....	3-8- مزایای همکاری سیستم های فازی با ماشین کرنل.....
68.....	4- سیستم های فازی مبتنی بر قانون
68.....	4-1- مقدمه.....
70.....	4-2- چرا از منطق فازی استفاده می شود.....
71.....	4-3- اصول منطق فازی.....
71.....	4-3-1- مجموع های فازی.....
75.....	4-3-2- توابع عضویت.....
81.....	4-3-3- عملگر های منطقی.....
83.....	4-3-4- قواعد اگر - آنگاه.....
86.....	4-4- استنتاج فازی.....
90.....	4-5- سیستم های استنتاج فازی.....
90.....	4-5-1- مقدمه.....
93.....	4-5-2- مدل های فازی ممدانی.....
94.....	4-5-3- استنتاج فازی به روش ساگینو.....

96.....	4-6-فرایند استنتاج فازی.....
96.....	4-6-1-پارامتر های ورودی فازی.....
98.....	4-6-2-بکارگیری عملگرفازی.....
99.....	4-6-3-بکارگرفتن روش استنتاج ضمنی.....
100.....	4-6-4-یکپارچه کردن خروجی ها.....
102.....	4-6-5-فازی زدایی.....
103.....	4-7-دسته بند الگو.....
103.....	4-8-سیستم های دسته بندی فازی تخمینی و توصیفی.....
105.....	4-8-1-سیستم های دسته بندی فازی مبتنی بر قانون.....
106.....	4-8-2-روش های تقسیم فضای الگو ها به زیر فضاهای فازی.....
109.....	4-8-3-قوانین فازی مورد استفاده برای عمل دسته بندی.....
110.....	4-8-4-تفاوت بین زیر فضاهای فازی و زیر فضا های غیر فازی.....
111.....	4-8-5-انتخاب کلاس در قوانین فازی.....
113.....	4-8-6-وزن دهی به قوانین فازی.....
114.....	4-8-7-تاثیر وزن دهی بر فضای تصمیم گیری در قوانین فازی.....
115.....	4-8-8-چندین روش شهودی تعیین وزن قوانین فازی.....
117.....	4-8-9-روش استنتاج در سیستمهای دسته بندی فازی.....
21.....	5-روش پیشنهادی :یک سیستم تشخیص نفوذ با استفاده از منطق فازی.....
121.....	5-1-مقدمه.....
122.....	5-2-مجموعه داده KDD99.....
123.....	5-2-1-دسته های مختلف درمجموعه داده KDDCup99.....

124	5-3-ویژگیها در مجموعه داده KDD99
126	5-4-نرمال سازی داده
126	5-5-توابع عضویت بکاررفته در روش پیشنهادی
127	5-6-نوع قوانین مورد استفاده در روش پیشنهادی دسته بندی فازی
128	5-7-روش انتخاب کلاس در قوانین فازی در روش پیشنهادی
129	5-8-استنتاج فازی مورد استفاده در روش پیشنهادی
130	5-9-چگونگی ساخت پایگاه قوانین
133	5-10-آموزش سیستم
134	5-11-آزمایش سیستم
137	5-12-نتایج آزمایش
140	5-13- یادگیری وزن قوانین
142	5-14- یادگیری بهترین نقطه عملیاتی در یک مسئله دو کلاسه
150	5-15-نتایج آزمایش پس از اعمال الگوریتم وزن دهی
153	5-16-بحث و گفتگو
156	5-17- نتیجه گیری
157	فهرست مراجع

فهرست شکل ها

عنوان

صفحه

- شکل 1-2-1-سیستم تشخیص نفوذ مبتنی بر رفتار غیر عادی.....15
- شکل 2-2-سیستم تشخیص نفوذ مبتنی بر سوء استفاده.....17
- شکل 1-3-مدل یک نرون عصبی.....40
- شکل 2-3-مدل همکار فازی – عصبی.....45
- شکل 2-4-مجموعه روزهای هفته.....72
- شکل 3-4-مجموعه روزهای آخر هفته.....73
- شکل 4-4-مقایسه دیدگاه دو ارزشی با چند ارزشی74
- شکل 5-4-مقایسه دید گاه دو ارزشی با چند ارزشی.....74
- شکل 6-4-مفهوم قد بلند و قد کوتاه از دیدگاه دو ارزشی.....76
- شکل 7-4-مفهوم قد بلند و قد کوتاه از دیدگاه چند ارزشی.....76
- شکل 8-4-1تابع عضویت مثلثی 2-تابع عضویت دوزنقه ای.....77
- شکل 9-4-1و2تابع عضویت گوسی و 3تابع عضویت ناقوس.....78
- شکل 10-4-تابع عضویت حلقوی.....79
- شکل 11-4-تابع عضویت حلقوی.....80
- شکل 12-4-عملگر های منطقی از دیدگاه دو ارزشی.....81
- شکل 13-4-عملگر های منطقی از دیدگاه چند ارزشی.....82
- شکل 14-4-ترکیب مجموعه فازی.....83

عنوان

صفحه

شکل 15-4 ترکیب بین دو ارتباط فازی.....	88
شکل 16-4- سیستم استنتاج فازی.....	91
شکل 17-4- نمودار سیستم استنتاج فازی.....	92
شکل 18-4- نقش عملگر در روش ساگینو.....	95
شکل 19-4- پارامتر های ورودی.....	97
شکل 20-4- بکار گرفتن عملگر فازی.....	98
شکل 21-4- بکار گرفتن عملگر استنتاج.....	99
شکل 22-4- بکار بردن روش جمع کردن.....	101
شکل 23-4- نتیجه فازی زدایی.....	102
شکل 24-4- قابلیت فهم در مقابل دقت در سیستم های تخمینی و توصیفی.....	105
شکل 25-4- یک نمونه از تقسیم بندی شبکه ای فازی 5×5 در فضای دوبعدی.....	106
شکل 26-4- توابع عضویت مختلف برای تقسیم بندی محور هر ویژگی.....	108
شکل 27-4- تولید قانون توسط یک داده در دو روش تقسیم بندی فازی و غیر فازی.....	111
شکل 28-4- تاثیر حذف یک قانون بر تقسیم بندی فضای الگوها.....	114
شکل 1-5- شمای از سیستم استنتاج فازی.....	129
شکل 2-5- تقسیم بندی متفاوت بردار هر خصیصه و معنای هر برچسب.....	130

فهرست جدول ها

عنوان	صفحه
جدول 4-5-5- ماتریس هزینه در KDD99.....	135
جدول 5-5-- ماتریس در آمیختگی.....	135
جدول 6-5-- مشخصات آماری داده های آموزشی و تست در KddCup99	138
جدول 7-5-- ماتریس هزینه جهت ارزیابی روشهای مختلف دسته بندی.....	138
جدول 8-5- تعداد قوانین فازی در مراحل مختلف.....	138
جدول 9-5- عملکرد مقایسه ای در چهار روش دسته بندی.....	139
جدول 10-5- مقدار CPE برای هر کدام از دسته بندها.....	139
جدول 11-5- ماتریس در هم آمیختگی برای یک دسته بند گسسته.....	142
جدول 12-5- الگوریتم یافتن بهترین حد آستانه.....	145
جدول 13-5- نتیجه روش دسته بندی با استفاده از قوانین بعد از وزن دهی.....	151
جدول 14-5- تعداد قوانین فازی در مراحل مختلف	151
جدول 15-5- عملکرد مقایسه ای در چهار روش دسته بندی.....	152
جدول 16-5- مقدار CPE برای هر کدام از دسته بند ها.....	152

فصل اول: مقدمه

1-مقدمه

استفاده از روشهای سیستم های تشخیص نفوذ امکان شناسایی کاربرانی که سعی به دسترسی غیر مجاز و یا تحریف و یا تخریب اطلاعات در شبکه های کامپیوتری مبتنی بر IP در بنگاههای تجارت الکترونیک را دارند فراهم می کند.

1-1 زمینه طرح مسئله

تهدید بر علیه داده های مشترک رو به افزایش است و بیشتر کمپانی ها بخاطر تهاجماتی که به سیستم های کامپیوتری آنها می شود متحمل ضررهای مالی هنگفتی می شوند. و مقدار زیادی از اطلاعات در معرض سرقت و تخریب قرار می گیرند. [1]

اطلاعات یکی از مهمترین دارایی هایی یک موسسه مالی یا بنگاه تجاری است. حفاظت از این دارایی جهت برقرار کردن و ایجاد اعتماد ما بین موسسه مالی و مشتریان و سازگار بودن با قوانین و در نگه داشتن شهرت و اعتبار بنگاه ضروری است. همچنین اطلاعات به موقع و قابل اعتماد جهت فرایند تعاملات و پشتیبانی از تصمیمات مشتری توسط بنگاه تجاری ضروری و اجتناب ناپذیر است. در صورتیکه اطلاعات توسط اشخاص غیرمجاز تغییر داده شود و یا در زمان نیاز به آن در دسترس نباشد. می تواند اعتبار و در آمد بنگاه تجاری و یا موسسه مالی را به خطر بیندازد. ظهور تکنولوژی ارتباطات و اینترنت امکان «اشتراک اطلاعات» و تبادل آسان اطلاعات را «بین سیستم های کامپیوتری» بوجود آورده است اطلاعات و فناوری های نوین بستری مناسب را برای انجام مبادلات تجاری و ارائه خدمات آنلاین مانند بانکداری الکترونیکی ، تجارت الکترونیکی و دولت الکترونیکی را ایجاد کرده است.

IT یک سکه دو روست: هم فرصت و هم تهدید می باشد اگر به همان نسبتی که به توسعه و همه گیری اش توجه و تکیه می کنیم به امنیت آن توجه نکنیم می تواند به سادگی و در کسری از ثانیه تبدیل به یک تهدید و مصیبت بزرگ شود.

تا اوایل دهه هفتاد فعالیت های مربوط به دسترسی و محافظت از اطلاعات در سازمانها و شرکت ها محدود به محل نگهداری این اطلاعات شامل آرشیو اسناد و شبکه های محلی کامپیوتری بود. در چنین محیط هایی با روشهای حفاظت فیزیکی امنیت سیستم ها و اطلاعات را تا حد بسیار بالایی تامین می کرد. اگر چه مزایای فضای تبادل اطلاعات غیر قابل انکار است ولی اتصالات سیستم های داخلی به شبکه های خارجی و بین المللی و ارائه خدمات و مبادله از طریق این شبکه ها خطرناک است و تهدیدات جدیدی را ایجاد کرده است. مهمترین نگرانی امنیتی مرتبط با سیستم های اطلاعاتی شامل دستیابی نفوذکنندگان به سیستم های اطلاعاتی و سرقت اطلاعات آنها ایجاد و قفه و اختلال در ارائه سرویسهای حیاتی و تغییر یا تخریب اطلاعات است و بدیهی است که در این شرایط روشهای حفاظت فیزیکی به تنهایی قادر به تامین امنیت نخواهد بود و سازمانها ناچار هستند روشهای جدید حفاظت اطلاعات و کنترل دسترسی منابع را در بنگاه تجاری بکارگیرند.

2-1- تاریخچه سیستم های تشخیص نفوذ

از دهه هشتاد میلادی سیستم های تشخیص نفوذ مورد بررسی قرار گرفت و از آن موقع به بعد تحقیقات و مقالات بسیاری در این خصوص تهیه و ارائه گردیده است. و تعدادی از سیستم های تشخیص نفوذ در هر دو بخش تجاری و آموزش ساخته شده است در گزارش فنی [2] اولین ایده درباره ثبت رویدادها که برای نظارت و کنترل تهدیدها می تواند مورد استفاده قرار بگیرد و تمام روشهای امنیتی مناسب را جهت ردگیری داده های مشکوک که از یک منبع با هویت ناشناس ارسال می شود را ارائه نموده است.

در [3] ایده تشخیص نفوذ بعنوان یک راه حل برای مشکلات حساس امنیتی در سیستم های کامپیوتری عنوان شده است. ایده اساسی این است که مهاجم دارای یک رفتار غیر نرمال در استفاده از کامپیوتر دارد سیستم تشخیص نفوذ با استفاده از رفتار یک کاربر عادی طرح ریزی می شود و هر گونه انحراف از آن به عنوان یک رفتار غیر عادی در نظر گرفته می شود. با روش های آماری¹ رفتار یک کاربر را در صورتیکه از رفتار عادی انحراف دارد به عنوان مهاجم می شناسد. این نوع از سیستم ها احتیاج به ساخت یک مدل از رفتار نرمال کاربر دارد. این روش سعی بر پیش بینی رویدادهای بصری از رویدادهایی کنونی دارد.

در [4] ساختار مبتنی بر مدل² را ارائه نمود که سعی در مدل کردن مهاجمین در سطحی بالاتر از ثبت رخدادهای نمونه ای با شکلی مجزا دارد این تکنیک با تکنیک سیستم خبره مبتنی بر قواعد سازی³ متفاوت است که سعی می کند به شکلی ساده از رویدادهای ثبت شده الگو برداری نماید.

در [5] آنالیز تغییر حالت⁴ را عنوان نمود. که رفتارهای مهاجم را که موجب یک سری تغییرات از حالت اولیه امنیتی به حالت مخاطره آمیز می شد به شکلی نموداری نمایش داد. استفاده کردن از وقایع ثبت رویدادها⁵ بعنوان ورودی، یک ابزار آنالیز است که در جهت مقایسه تغییر حالت کاربران با نمودار هایی که از تغییرات حالت در حمله های شناخته شده موجود است بکار گرفته می شود.

تکنیکهای علائم هشدار دهنده کلیدی⁶ از علائم هشدار دهنده کلیدی کاربر برای تعیین تلاشهای تهاجم گرانه استفاده می کند. در این روش ساختار اصلی تشکیل شده است از

¹ . statically approaches
² . model-based approach
³ . rule-based expert system
⁴ . state transition analysis approach
⁵ . audit trial
⁶ . keystroke monitoring technique

الگوهای که دارای نتایجی بوده اند که منجر به علائم هشدار دهنده شده است و تعدادی از آنها به عنوان علائم هشدار دهنده کلیدی مهاجم شناخته می شود.

در [6] ساختار انطباق الگویی¹ ارائه شده است. در این روش علامت مشخصه مهاجم ها را شناسایی و به صورت رمز در می آید. به صورتی که الگوها دائما خود را با داده های ثبت شده تطبیق دهند. علامت مشخصه ای که الگوبندی شده اند دائما با داده ها مقایسه می شوند و هر داده ای که منطبق با علامت مشخصه بود به عنوان مهاجم شناخته می شوند در سالهای اخیر چندین پایگاه داده از سیستم های تشخیص نفوذ ترکیبی ارائه شده است.

در [7] ایده معماری جدیدی را عنوان کرد که هر دو روشهای سیستم تشخیص نفوذ مبتنی بر رفتارهای غیر نرمال و سوء استفاده² را شامل می شد و سیستم تصمیم گیرنده پشتیبان که ترکیب کننده نتایج هر دو روش می باشد را مورد استفاده قرار داد. مدل تشخیص نفوذ مبتنی بر رفتارهای غیر نرمال از ساختار نقشه خودسازماندهی³ برای مدل سازی رفتار نرمال استفاده می کند. مدل تشخیص نفوذ مبتنی بر سوء استفاده از یک الگوریتم درختی تصمیم⁴ برای دسته بندی انواع مختلف مهاجم استفاده می کند. یک سیستم پشتیبان تصمیم مبتنی بر نقش سازی⁵ نتایج حاصل از مدل های مبتنی بر سوء استفاده گر را در رفتار غیر نرمال با همدیگر ترکیب می کند.

¹ . pattern matching approach

² .misuse

³ . self organizing map (SOM)

⁴ . decision tree algorithm

⁵ . Decision support system ((DSS)) agent architecture